UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

JUDITH RAANAN *et al.*,	
Plaintiffs,	
-v-	Case No: 1:24-cv-00697-JGK
BINANCE HOLDINGS LIMITED, and CHANGPENG ZHAO,	**ORAL ARGUMENT REQUESTED**
Defendants.	

PLAINTIFFS' MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS THE FIRST AMENDED COMPLAINT

SEIDEN LAW LLP
Robert W. Seiden
Amiad Kushner
Jake Nachmani
Jennifer Blecher
Dov Gold
322 Eighth Avenue, Suite 1200
New York, NY 10001
(212) 523-0686

PERLES LAW FIRM, P.C.
Steven R. Perles
Joshua K. Perles
Edward B. MacAllister
816 Connecticut Avenue, NW
12th Floor
Washington, D.C. 20006
(202) 955-9055

Attorneys for Plaintiffs

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Rules and Statutes

Plaintiffs submit this memorandum of law in opposition to Defendants Binance Holding Limited ("Binance") and Changpeng Zhao's ("Zhao"; and collectively with Binance, "Defendants") motion to dismiss the First Amended Complaint (ECF 17, "Motion").[1]

PRELIMINARY STATEMENT

Defendants enabled Hamas and PIJ. While Hamas and PIJ committed the horrific October 7 Attacks, Defendants were their knowing and deliberate financial enablers. Plaintiffs are U.S. individuals and their family members who were brutally murdered or injured in the Attacks. Seeking justice, Plaintiffs bring claims under the ATA for aiding and abetting and primary liability against Defendants, whose dangerous and unique provision of financial services to Hamas and PIJ substantially contributed to the Attacks.

The FAC states these claims. Defendants intentionally created the Binance platform as an illicit financial tool for criminal activity, knowingly operated the platform without KYC and AML controls, and knowingly provided their criminal and terrorist customers access to digital currency that was designed to evade regulation and hide their tracks. In the post-9/11 world, preventing terrorists from accessing financial markets is of paramount concern for any responsible financial institution, but Defendants sought to attract criminals and terrorists to their platform. Foreseeably, Hamas, PIJ, and their affiliates transacted on Binance. Moreover, and notwithstanding their regulatory obligations to report suspicious or illegal activity, Defendants affirmatively misled regulators about Hamas and PIJ's activities on Binance, obscuring their financing and blocking possible government investigations years before the Attacks.

[1] Capitalized terms not defined herein have the same meanings as ascribed to them in the First Amended Complaint ("FAC"). References to "¶" and "Mot." are to paragraphs of the FAC and Defendants' memorandum of law in support of their Motion to Dismiss (ECF 19), respectively. References to "Raanan Decl." and "Ludmir Decl." are to the declarations of Uri Raanan and Jeffrey Ludmir, respectively, filed contemporaneously herewith. All emphasis is added; all internal quotations and citations are omitted.

Defendants knowingly did this. Defendants' regulators concluded that, prior to the Attacks, Defendants knew Hamas, PIJ, and their affiliates were transacting on Binance. Defendants' internal communications—epitomized by jokes and deliberate indifference—demonstrate this.

These terrorists' preference for cryptocurrency was widely known. Hamas publicly requested funding via Binance. The media widely reported on it. Israel's counter-terrorism financing agency seized and publicized Hamas and PIJ crypto-wallets. Binance's competitor published a how-to-guide for crypto-platforms to detect terrorist usage.

As a result of Defendants' deliberate design and affirmative misconduct, Hamas and PIJ transacted in massive amounts on Binance. Based on publicly available information, Plaintiffs uncovered $101 million in transactions by these groups leading up to the Attacks. The actual amount transacted by Hamas and PIJ is known by Defendants and recorded on their internal ledger.

Defendants seek dismissal on numerous grounds, all of which fail. Defendants argue that *Twitter* requires dismissal. However, in *Twitter*, the digital platforms were largely passive and indifferent to their users' content, and the platforms had no legal duties regarding that content. Here, Defendants designed a platform specifically to facilitate criminal financing, knew that specific terrorist organizations, including Hamas and PIJ, were using their platform, and took proactive steps to conceal that criminal activity and deceive regulators, thereby allowing these terrorists to continue transacting on the platform.

Defendants also contend that the FAC does not allege that they knew that Hamas and PIJ transacted on Binance, and, even so, the small number of alleged transactions did not cause Plaintiffs' injuries. The contents and conclusions of U.S. government investigations, among other allegations, show otherwise. Defendants' standing and jurisdictional arguments also fail.

The FAC alleges Plaintiffs' claims; Defendants' Motion should be denied.

THE FAC'S ALLEGATIONS

Plaintiffs

Plaintiffs are U.S. citizens and their family members who were killed, tortured, taken hostage, or otherwise harmed in the horrific October 7, 2023 Hamas and PIJ terrorist attacks ("Attacks"). ¶¶19-64. Plaintiffs bring claims under the ATA via 18 U.S.C. § 2333(d)(2), 18 U.S.C. §§ 2339A and 2339B against Defendants for supporting the Attacks. ¶¶247-85.

FTO Crypto-Financing Breaks Into Public View

Binance is a cryptocurrency platform and exchange. ¶139. On Binance, users can open accounts and transact in various cryptocurrencies and fiat currencies.[2] ¶140. Zhao was Binance's founder and CEO, who, though he was forced to resign, still retains ownership and control of Binance. ¶¶8, 180. Binance conducted extensive business in the U.S. and in New York. ¶¶154-58.

Hamas and PIJ are violent terrorist organizations long designated by the U.S. as Foreign Terrorist Organizations ("FTOs") due to decades of terrorism against U.S nationals. ¶¶76-85.

Hamas and PIJ cannot openly access traditional financial markets and must raise money in clandestine ways, for which cryptocurrency is tailor-made. ¶132. Hamas has openly used crypto since 2019 when it encouraged its followers to donate with Bitcoin. ¶¶134-35. Also in 2019, Hamas publicly sought crypto-donations from its supporters, ***identifying Binance as a platform.*** ¶¶201-02. Through 2023, Hamas continued to openly request crypto-funding. ¶¶203-04.

Between 2019 and the Attacks, the media, including PBS, *The Wall Street Journal*, and Israel-based journalists, widely reported on terrorist-financing via cryptocurrency, including Hamas. ¶¶203-07. In 2021, Binance's crypto-platform competitor, Coinbase, published a report on best practices for identifying and reporting terrorist-financing activity on platforms. ¶208.

[2] Fiat currencies are government-issued currencies that are not backed by a commodity such as gold, *e.g.* U.S. dollars.

Governments also caught on and took enforcement actions against FTOs and their affiliates for their crypto-transactions. In June 2021, Israel's National Bureau for Counter-Terrorism Financing ("NBCTF") publicly seized Hamas-affiliated crypto-wallets, *e.g.*, BuyCash, a Gaza-based financial services entity. ¶¶195-96, 226. In March 2022 and April 2023, the NBCTF publicly seized wallets used of Dubai Co., another Gaza-based entity, that were used to transact with Hamas. ¶¶195, 197, 226. In July 2023, the NBCTF publicly seized PIJ's crypto-wallets.[3] ¶226.

Defendants Created The Perfect Financing Tool For Terrorists

As a money services business ("MSB") conducting business in the U.S., Binance was subject to laws meant to identify and prevent illegal activity. ¶¶158-73. Binance was required to establish a robust anti-money laundering program ("AML"), perform due diligence and know-your-customer ("KYC") investigations on its users, and file Suspicious Activity Reports ("SARs") with FinCEN as to activities Binance knew or suspected were illegal. ¶¶160, 17-72.

Instead, Defendants created and operated a unique financial platform on which criminals could access global markets, while keeping their activities hidden from government scrutiny. ¶¶174-92. In Zhao's own words from June 2019, he did not want to "***be held accountable***" to regulators. ¶176. Also in June 2019, Binance's Chief Compliance Officer referred to Binance's business model as "***the international circumvention of KYC***," so that Binance could "***reduce the losses to ourselves, and … make the U.S. regulatory authorities not trouble us***." ¶177.

[3] A cryptocurrency wallet is a device or program that stores cryptographic keys to transact cryptocurrency. ¶¶140, 143. Wallets contain a unique address that allows third-parties to track that wallet's transactions. ¶¶140, 143. This data is stored publicly on a given cryptocurrency's "ledger" but is made pseudonymous by use of said addresses. ¶¶143-44. Associating an address with a known identity, such as Hamas, reveals the wallet's transactions in a particular cryptocurrency. ¶¶144-45. Thus, it is often said that cryptocurrency is pseudonymous not anonymous. ¶¶144-45. However, an account-holder can move cryptocurrency from a wallet into a Binance "omnibus" wallet, a pseudonymous transaction recorded on the cryptocurrency ledger. ¶¶140, 145, 153. The account-holder is then credited on Binance's private ledger and can transact on Binance's exchange—these transactions proceed anonymously to external observers but are known to Binance. ¶¶145, 153. This process is inverted to withdraw cryptocurrency from a Binance account. ¶143.

Defendants effectuated their international circumvention of KYC/AML in a variety of ways. They intentionally mischaracterized their users' locations, advised their users to install IP-blocking software, and falsified KYC data. ¶180. Moreover, from its start-up in 2017 through 2021, Binance allowed users to open accounts with ***no KYC whatsoever*** and allowed users to open multiple accounts so they could bypass daily transaction limits for single accounts. ¶183. When Binance began conducting nominal due diligence on its users, ***four years after its start-up,*** Binance intentionally loopholed this process, ***allowing existing users to continue using the platform without submitting any KYC***. ¶184.

Foreseeably, as a result of Defendants' international circumvention of KYC, criminals used Binance. And Defendants knew it. In 2020, Binance's CCO, in response to having been presented with evidence of criminal transactions on Binance, admitted that criminals were using the platform, stating "***Like come on. They are here for crime***." ¶187. Binance's Money Laundering Reporting Officer agreed, commenting "***we see the bad, but we close 2 eyes***." ¶187. Another compliance officer sought to advertise Binance to drug cartels, stating "we need a banner '***is washing drug money too hard these days - come to binance we got cake for you***.'" ¶188.

Defendants Knowingly Provided Financial Services To Terrorists

Foreseeably, Hamas, PIJ, and their affiliates transacted on Binance. FinCEN concluded that from July 2017 through July 2023, Defendants' "***willfull failure***" to implement an AML program "***directly led to the platform being used to process transactions related to … terrorist financing***" (¶190) ***and that such financing was related to Hamas and PIJ***. ¶¶211-12. FinCEN and the CFTC concluded that ***Hamas operated on Binance in February 2019***. ¶¶213, 216. Binance's own KYC provider identified Hamas usage on Binance ***at least twice – in April 2019 and in July 2020***. ¶¶213, 215.

Because of the risk of illicit finance associated with the pseudonymity of cryptocurrency, it was incumbent on Defendants to engage in effective KYC. Defendants had access to transaction monitoring tools for KYC/AML, including tools that pinpoint a wallet's source and destination of funds. ¶¶146-150. But Defendants intentionally circumvented KYC/AML procedures and took steps to ensure that Hamas and PIJ's transactions would remain hidden from regulators. FinCEN concluded that ***between July 2017 and July 2023, Binance failed to file SARs regarding dozens of Hamas and PIJ transactions "associated with terrorist financing."*** ¶¶211-12, 214-16. FinCEN also concluded that "***Binance was aware of extensive suspicious activity involving [BuyCash] – including connections [] to terrorist organizations***." ¶218. Zhao admitted that Defendants' practice of misleading regulators would foster terrorism financing on Binance, stating in June 2019: "***the U.S. has this law: you have to prevent … terrorists from doing any transactions. In order [for America] to accomplish this … you have to give your data to the American regulators***." ¶221. Defendants also pressured their own KYC service provider (who had identified Hamas transactions) to mislead regulators about these transactions. ¶214. In July 2020, instead of freezing accounts and filing SARs, Binance's former COO instructed compliance personnel to let a customer—***flagged as associated with Hamas***—this time leave with his funds, and to tip him off that he had been identified as a Hamas associate. ¶¶5, 214.

Terrorists Transacted In Massive Amounts On Binance

Leading up to the Attacks, Defendants' misconduct allowed terrorists to transact in massive amounts on Binance. With just publicly available data, Plaintiffs uncovered ***$60 million in Hamas and PIJ transactions*** (¶¶194, 209), ***$25 million in BuyCash transactions*** (¶196), and ***$16 million in Dubai Co. transactions***. ¶¶197. Accordingly, Plaintiffs uncovered no less than ***$101 million in terrorist and terrorist-affiliated transactions leading up to the Attacks***. ¶199.

ARGUMENT

I. THE FAC STATES AN AIDING AND ABETTING CLAIM

Defendants challenge aiding and abetting liability under 18 U.S.C. § 2333(d)(2), contending that the FAC does not allege that Defendants "knowingly and substantially assist[ed] the principal violation" or that they were "generally aware" of their role in the "overall illegal or tortious activity." *Twitter, Inc. v. Taamneh*, 598 U.S. 471, 486 (2023). The FAC alleges both.[4]

A. The FAC Alleges Knowing And Substantial Assistance

Knowing, substantial assistance is alleged where "the defendant consciously and culpably participate[d] in a wrongful act so as to help make it succeed." *Twitter,* 598 U.S. at 493.

1. Defendants' Conscious And Culpable Participation

A routine services provider is culpable if it provides services "***in an unusual way***" or "***provides such dangerous wares*** that selling those goods to a terrorist group could constitute aiding and abetting a foreseeable terrorist attack." *Id.* at 502. The FAC establishes both.

First, Defendants' creation and operation of the Binance platform was unusual *and* dangerous because Defendants intentionally created an illicit financing tool designed to hide criminal activity. Defendants' business strategy was in their words: the "***international circumvention of KYC***." ¶177. Notwithstanding their legal obligations to disclose illegal activity (¶221), Defendants used their fake compliance program to enable terrorist financing. ¶¶174-99, 215-19. And even when Binance initiated due diligence, ***four years after its start-up***, Defendants' meager KYC protocol was deliberately useless. ¶¶178, 180-81. Binance wanted profits from criminal enterprises; as an employee stated in 2019, *"we need a banner '****is washing drug money***

[4] A court "must accept as true all nonconclusory factual allegations in the complaint and draw all reasonable inferences in the Plaintiffs' favor." *Kaplan v. Lebanese Canadian Bank, SAL*, 999 F.3d 842, 854 (2d Cir. 2021). The inquiry is whether "***all*** of the facts alleged, taken collectively" permit a relevant inference, not whether "any individual allegation, scrutinized in isolation" does. *Tellabs, Inc. v. Makor Issues & Rts., Ltd.*, 551 U.S. 308, 322-23 (2007).

too hard these days - come to binance we got cake for you.'" ¶188. Defendants' operation of Binance constitutes affirmative misconduct, not "passive nonfeasance." *Twitter*, 598 U.S. at 500.

Second, Hamas and PIJ transacted on the platform. FinCEN concluded that from July 2017 through July 2023 "***Binance's willful failure*** to implement an effective [AML] program" ***directly led to Hamas and PIJ*** transactions in "***significant sums***." ¶¶5, 190, 211-12. FinCEN and the CFTC concluded that ***Hamas operated on Binance in February 2019***. ¶¶213, 216. Binance's own KYC provider identified Hamas usage ***at least twice – in April 2019 and July 2020***. ¶¶213, 215. Plaintiffs themselves uncovered ***$60 million in Hamas and PIJ transactions on Binance***. ¶194.

Third, Defendants affirmatively helped terrorist-users evade government investigation, giving them "special treatment." *Twitter*, 598 U.S. at 498. Notwithstanding their duty to report illegal or suspicious activities on the platform, ***between July 2017 and July 2023, Binance concealed Hamas and PIJ transactions by systematically failing to file SARs*** and continued to do business with them. ¶¶5, 211-12, 214-16. Likewise, FinCEN found that Binance failed to file SARs as to Hamas-affiliate BuyCash, even though "***Binance was aware of extensive suspicious activity involving [BuyCash] – including connections [] to terrorist organizations***." ¶218. Defendants also pressured their provider (who had identified Hamas transactions) to mislead regulators about these transactions. ¶214. In July 2020, instead of freezing accounts and filing SARs about a user ***flagged as a Hamas associate***, Binance's former COO instructed compliance personnel to let the user leave with his funds and warn him about being flagged. ¶5.

And *fourth*, Defendants knew they were substantially assisting Hamas and PIJ. Defendants' systemic failure to report terrorist transactions via SARs demonstrates ***Defendants' knowledge in real time that these entities were transacting on Binance***. FinCEN's conclusion as to Binance's knowledge of the BuyCash transactions' connections to terrorism is clear. ¶218. Likewise,

Defendants' internal communications show their knowledge. In February 2019, Binance's CFO demonstrated his knowledge of terrorists' presence on the Binance platform and acknowledged the possibility that they were using it to buy weapons. ¶216. In June 2019, ***Zhao admitted*** that Defendants' intentional concealment of terrorist transactions would foster terrorist financing, stating that, under the law, "***to prevent … terrorist from doing any transactions … you have to give your data to the American regulators.***" ¶221. In 2020, Binance's CCO responded to evidence of criminal transactions by stating: "***Like come on. They are here for crime***"; and Binance's Money Laundering Reporting Officer commented: "***we see the bad, but we close 2 eyes***." ¶187.

Defendants maintain that this case is on "all fours" with *Twitter.* Mot. 16. But there, the Supreme Court recognized Twitter and YouTube ("*Twitter* Platforms") to be online content publishing platforms on which people "can sign up for… and start posting content … ***without much (if any) advance screening by defendants***." *Twitter*, 598 U.S. at 480. As such, the *Twitter* Platforms' relationship to their users is "***passive***" and "***largely indifferent,***" and, as "communications provider[s]," they are like "cell phones, email, or the internet []." *Id.* at 499-500.

This case is not like *Twitter* because, unlike the *Twitter* Platforms, Defendants engaged in years of knowingly directed affirmative misconduct. *Twitter* offers no protection for providers of even "routine services" where they do so "in an unusual way," such as when a morphine distributor mailed narcotics "far in excess of normal amounts" to a customer. *Id*. at 502. Unlike the *Twitter* Platforms, the law required Binance to conduct vigilant due diligence on its users, but its deliberately defective diligence produced callous jokes instead of the required SARs. In the world of financial service providers, this was an aberrant, criminal, and dangerous way to do business.

Also, Defendants' culpability inherently exceeds that of recent Second Circuit precedent because of the unique nature of the platform. *See, e.g.*, *Kaplan*, 999 F.3d at 866 (concealing FTO

transactions and circumventing terrorism sanctions); *Bartlett v. Societe Generale de Banque Au Liban SAL*, 2020 WL 7089448, at *12 (E.D.N.Y. Nov. 25, 2020) (providing access to financial markets and accounts). Unlike traditional banking, Binance's business hinged on the anonymous and pseudonymous portions of the crypto ledger, tailormade for terrorism finance. ¶¶143-44, 227.

2. The Nexus Between Defendants' Assistance And The Attacks

While *Twitter* requires a "nexus" between the Defendants' assistance and the terrorist act (598 U.S. at 503), it also recognizes that a defendant "***can be held liable for other torts that were a foreseeable risk of the intended tort***." *Id.* at 496. A "close nexus" is ***not*** required and "even more remote support can still constitute aiding and abetting." *Id*.

The FAC alleges this, as Defendants were systemic financial enablers of Hamas and PIJ. For years, Defendants provided these terrorists with the ability to transact millions of dollars in crypto and access global markets, even after they had been identified. Moreover, Zhao admitted the connection between Defendants' assistance and a future terror attack. ¶221; *see King v. Habib Bank Ltd.*, 2023 WL 8355359, at *3 (S.D.N.Y. Dec. 1, 2023) (provision of banking services to terrorists and their allies satisfied nexus because attack was foreseeable consequence of services); *Bonacasa v. Standard Chartered PLC*, 2023 WL 7110774, at *11 (S.D.N.Y. Oct. 27, 2023) (same).

Defendants maintain that the FAC must show that Defendants' financial services were used for the Attacks. Mot. 17. But *Twitter* rejects this contention. *See* 598 U.S. at 497 ("strict nexus" not required; "remote support can still constitute aiding and abetting"); *see also Bonacasa*, 2023 WL 7110774, at *9 (nexus "even where the defendant did not intentionally aid the specific terrorist attack itself."). And for good reason: financial support to an organization like Hamas "if not used directly, arguably would be used indirectly by substituting it for money in Hamas' treasury; money

transferred by Hamas' political wing in place of the donation could be used to buy bullets." *Gill v. Arab Bank, PLC*, 893 F. Supp. 2d 474, 507 (E.D.N.Y. 2012).

3. The *Halberstam* Factors Confirm Defendants' Substantial Assistance

The six factors in *Halberstam v. Welch*, 705 F.2d 472 (D.C. Cir. 1983) "capture the essence of aiding and abetting." *Twitter*, 598 U.S. at 504. These factors are "variables," and the "absence of some need not be dispositive." *Kaplan*, 999 F.3d at 856. The FAC establishes them.

Nature of the Act: Defendants' provision of financial services to an FTO is "***indisputably important***." *Halberstam*, 705 F.2d at 488; *see also Zobay v. MTN Grp. Ltd.*, 695 F. Supp. 3d 301, 349 (E.D.N.Y. 2023) ("[f]inancial support is indisputably important to the operation of a terrorist organization … ***any money provided … may aid its unlawful goals***.").

Amount of Assistance: Contrary to Defendants' assertion (Mot. 18), Plaintiffs do not need to trace Defendants' financial services to the Attacks; tracing "specific dollars to specific attacks … would be impossible and would make the ATA practically dead letter[.]" *Strauss v. Credit Lyonnais, S.A.*, 925 F. Supp. 2d 414, 433 (E.D.N.Y. 2013).

As to the quantum of assistance, the $60 million transacted by Hamas and PIJ and the approximately $100 million transacted by FTO and FTO-affiliated wallets leading up to the Attacks (¶¶193-98) is more than sufficient to satisfy this factor. *See Bonacasa*, 2023 WL 2390718, at *14 ($25 million in loans was substantial assistance); *Bartlett*, 2020 WL 7089448, at *15 (same as to "processing millions of dollars in transfers" for FTO).

Defendants' Presence: The tortious enterprise in *Halberstam*, as here, required activities in different locations. *See* 705 F.2d at 488. The Attacks required substantial funding (¶¶124, 132-38), "which can be expected to occur far earlier and away from the where the Attacks were

committed." *Bartlett*, 2020 WL 7089448, at *13; *see also Zobay*, 695 F. Supp. 3d at 350 (the "ongoing business relationship" demonstrated "transactional[]" presence).

Relationship to Hamas/PIJ: A "direct relationship between the defendant and the FTO is not required[.]" *Honickman v. BLOM Bank SAL*, 6 F.4th 487, 501 (2d Cir. 2021). A "commercial relationship," even if "indirect" to an FTO, is sufficient so long as the assistance provided is substantial. *Averbach v. Cairo Amman Bank*, 2022 WL 2530797, at *16 (S.D.N.Y. Apr. 11, 2022). The FAC exceeds this by alleging that Hamas and PIJ were Defendants' customers (¶¶212-16) and that Binance conducted approximately $60 million in direct transactions with Hamas and PIJ cryptocurrency wallets. ¶¶3, 194, 209, 226-27.

State of Mind: This factor concerns a "long-term intention to participate in an ongoing illicit enterprise." *Halberstam*, 705 F.2d at 488. Defendants' actual knowledge that Hamas and PIJ operated on the Binance platform for years (*see supra* Section I.A.1) and their general awareness of their role in Hamas and PIJ's terrorism financing (*see infra* Section I.B) are sufficient. *See Bartlett*, 2020 WL 7089448, at *14 (allegations establishing general awareness satisfied state of mind); *Averbach*, 2022 WL 2530797, at *16 (state of mind satisfied because bank-defendant was aware it was "enabling fundraising for Hamas's terror activities").

Duration of Assistance: This factor assesses "the length of time an alleged aider-abettor has been involved with a tortfeasor" and the "quality and extent of their relationship[.]" *Halberstam,* 705 F.2d at 484. Defendants maintained relationships with the FTOs and their affiliates for years leading up to the Attacks; this is sufficient. ¶¶193-98, 209-13; *see Bonacasa*, 2023 WL 2390718, at *14 (providing services for a "significant period" of time up to attack); *Averbach*, 2022 WL 2530797, at *17 (multi-year relationship with FTO-affiliates).

B. The FAC Alleges Defendants' General Awareness

General awareness is not "full recognition"; it connotes "something less than full, or fully focused, recognition." *Kaplan*, 999 F.3d at 863. Because a plaintiff "cannot be expected to plead a defendant's actual state of mind," a complaint may "contain general allegations as to a defendant's knowledge[.]" *Id.* at 864. At this stage, a plaintiff does not need to allege a defendant "knew or should have known" facts concerning public sources of information, just that the information was made public. *Honickman*, 6 F.4th at 501. When a defendant assists an FTO, general awareness is established if the defendant was generally aware of its role in "an overall illegal activity" from which an "act of international terrorism was a foreseeable risk." *Kaplan*, 999 F.3d at 860. When a defendant provides assistance to an FTO's intermediaries, general awareness is established if those intermediaries "were so closely intertwined with [the FTO's] violent terrorist activities that one can reasonably infer that [the defendant] was generally aware … that it was playing a role in unlawful activities from which the [terrorist attack was] foreseeable." *Id.* at 861.

The FAC meets both standards. Defendants provided financial services directly to Hamas and PIJ. ¶¶172, 194, 211-12, 216-18. Where Defendants serviced intermediaries, such as BuyCash and Dubai Co., the FAC identifies the public notice establishing these entities' connections to Hamas. ¶¶195-97, 209, 218, 226. This is more than sufficient. *See Averbach*, 2022 WL 2530797, at *12 (Israel's designating bank's customers as Hamas fronts were "red flags" that customers "were closely intertwined with Hamas" contributing to a "plausible inference" that defendant-bank "was generally aware it was assisting unlawful activities of Hamas").

The FAC establishes Defendants' general awareness in other ways. *First,* Defendants knew they functioned as financial enablers of criminals and terrorists, as demonstrated by the internal communications among Binance's "compliance staff." *See supra* Section I.A; ¶¶174-92, 210-13.

Second, the FAC establishes Defendants' general awareness by alleging widespread public knowledge of Hamas' goals (¶¶76-81), and, between 2019 and 2023, Hamas' publicized use of cryptocurrency and donations via Binance. ¶¶201-03. At the pleading stage, plausible inferences regarding general awareness may be drawn from public statements. *See Honickman*, 6 F.4th at 501; *Averbach*, 2022 WL 2530797, at *10 (general awareness based on Hamas' "public and widely reported" calls for violence and recruitment of individuals to commit violence); *Henkin v. Kuveyt Turk Katilim Bankasi, A.S.*, 495 F. Supp. 3d 144, 157 (E.D.N.Y. 2020) (defendant did not have to know public information for it be imputed).

Likewise, and further supporting Defendants' general awareness, media and third parties covered Hamas' use of crypto and Binance. *See Kaplan*, 999 F.3d at 862; *Bartlett*, 2020 WL 7089448, at *10. In 2019, the Israeli press reported on Hamas' use of Binance, and a crypto-analytics firm, via its public Twitter page, flagged Hamas' use of the platform. ¶205. In June 2021, *The Wall Street Journal* reported on Hamas' extensive cryptocurrency use. ¶206. Binance's competitor published a report for crypto-platforms to detect terrorist usage. ¶208.

Israel, through enforcement actions, publicly announced Hamas, PIJ, and their affiliates' use of crypto. In June 2021, Israel's NBCTF publicized BuyCash wallets used to transfer funds to Hamas. ¶¶196, 209. In March 2022 and April 2023, the NBCTF publicized Dubai Co. wallets. ¶226. Defendants' general awareness also stems from these designations. *See Kaplan*, 999 F.3d at 864 ("it would defy common sense" that government designations of terrorist-fronts would not support general awareness); *Henkin*, 495 F. Supp. 3d at 160 ("it would defy credulity" that a bank required to have AML policy would be "oblivious" to designations by Israel).

Third, the FAC alleges Defendants' general awareness based on the magnitude of Hamas and PIJ transactions. *See Averbach*, 2022 WL 2530797, at *13 (transfers were "red flag[s]").

II. THE FAC STATES PRIMARY LIABILITY CLAIMS

The ATA provides for liability for "[p]roviding material support to terrorists" and to "designated foreign terrorist organizations." 18 U.S.C. §§ 2339A, 2339B.

A. The FAC Alleges An Act Of International Terrorism

The ATA provides for liability where a plaintiff is injured "by reason of an act of international terrorism." 18 U.S.C. § 2333(a). "[I]nternational terrorism" are activities that: (i) "involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State" and (ii) "appear to be intended" to "intimidate or coerce a civilian population," "influence the policy of a government by intimidation or coercion," or "affect the conduct of a government by mass destruction, assassination, or kidnapping." 18 U.S.C. § 2331(1)(A)-(B). A violation of § 2339A for "[p]roviding material support to terrorists" or of § 2339B for providing material support to a "foreign terrorist organization" qualifies as "a violation of the criminal laws" under § 2331(1)(A) and triggers civil liability under the ATA.

1. Acts Dangerous To Human Life

"Giving money to Hamas … is an act dangerous to human life." *Boim v. Holy Land Foundation for Relief and Development*, 549 F.3d 685, 690 (7th Cir. 2008). "Providing financial services … is also dangerous to human life since financial services increase Hamas' ability to carry out attacks in the same way[.]" *Miller v. Arab Bank, PLC*, 372 F. Supp. 3d 33, 45 (E.D.N.Y. 2019).

Defendants committed acts dangerous to human life through their provision of unusual and dangerous crypto-financing services to Hamas and PIJ. *See supra* Section I.A; *Schansman v. Sberbank of Russia PJSC*, 565 F. Supp. 3d 405, 416 (S.D.N.Y. 2021) (facilitation of funding to FTO affiliates was dangerous to human life); *Lelchook v. Islamic Republic of Iran*, 393 F. Supp. 3d 261, 266 (E.D.N.Y. 2019) (routing payments on behalf of FTO was dangerous to human life).

2. Objective Intent To Intimidate Or Coerce

Whether a defendant appeared "to have intended its activities to intimidate or coerce is … a question of what its intent objectively appeared to be." *Weiss v. Nat'l Westminster Bank, PLC.*, 993 F.3d 144, 161 (2d Cir. 2021). "To require proof that the [defendant] intended that his contribution be used for terrorism—to make a benign intent a defense—would as a practical matter eliminate [ATA] liability except in cases in which the [defendant] was foolish enough to admit his true intent." *Boim*, 549 F.3d at 698–99.

Defendants' objective intent is set forth by their knowing, substantial assistance and general awareness. *See supra* Sections I.A.1, I.B; *Lelchook*, 393 F. Supp. 3d at 266 (intent by routing money to FTO affiliates); *Wultz v. Islamic Republic of Iran*, 755 F. Supp. 2d 1, 49 (D.D.C. 2010) (intent because bank executed transactions after knowing they were on behalf of PIJ).[5]

B. The FAC Alleges Defendants' Scienter

Under § 2339A, a complaint must allege that a defendant knew or intended its services would "generally facilitate the terrorist activities." *Id.* at 46. Under § 2339B, a complaint must allege defendant's "knowledge of the organization's connection to terrorism." *Weiss*, 993 F.3d at 164. "Deliberate indifference" – whether a defendant "knows there is a substantial probability that [an FTO] engages in terrorism but ... does not care" – is sufficient. *Id.* at 208.

Defendants' deliberate indifference is pled by the FAC's allegations that Defendants knew that Hamas and PIJ (and their intermediaries) transacted on Binance leading up to the Attacks (Section I.A.1) and Defendants' general awareness of their role in Hamas and PIJ's activities (Section I.B). *See Schansman*, 565 F. Supp. 3d at 417 (deliberate indifference established by

[5] Defendants' cited authorities (Mot. 12-13) are inapplicable. *See, e.g.*, *Weiss*, 993 F.3d at 162 (stands for the neutral principle that a plaintiff must plead all of the statutory elements of §§ 2339A and 2339B); *Stutts v. De Dietrich Grp.*, 2006 WL 1867060, at *2 (E.D.N.Y. June 30, 2006) (no factual allegations regarding knowledge); *O'Sullivan v. Deutsche Bank AG*, 2019 WL 1409446, at *7-8 (S.D.N.Y. Mar. 28, 2019) (no basis to connect affiliates to FTOs).

allegations concerning terrorist group's public fundraising, media's publicizing group's violence, and government investigations); *Goldberg v. UBS AG*, 660 F. Supp. 2d 410, 433-34 (E.D.N.Y. 2009) (scienter where public sources identified bank's customers as Hamas intermediaries).

Defendants contend that their provision of "routine services" to persons or entities "with connections to terrorist organizations—as opposed to the organizations themselves" cannot as a matter of law give rise to claims under §§ 2339A and 2339B. Mot. 13. However, Defendants ignore the FAC's allegations which show that Defendants knowingly provided services directly to Hamas and PIJ—there is nothing routine about that. *See supra* Sections I.A.1, I.B. Moreover, ***liability attaches to a defendant who provides material support to FTOs through those FTOs' intermediaries***. *See supra* Sections II.A.1-2; *Sokolow v. Palestine Liberation Org.*, 60 F. Supp. 3d 509, 522 (S.D.N.Y. 2014) ("direct connection between providing material support to the [FTO] and injury to Plaintiffs is not required"; "attenuated connection" suffices).

C. The FAC Alleges Causation

Proximate cause is shown where a defendant's conduct was a "substantial factor" such that plaintiff's injury was "reasonably foreseeable or anticipated[.]" *Rothstein v. UBS AG*, 708 F.3d 82, 92 (2d Cir. 2013). Plaintiffs' injuries were the foreseeable consequences of Defendants' material support. *See supra* Sections I.A.1, I.A.3. To support their operations and execute the Attacks, Hamas and PIJ publicized their use of cryptocurrency and Binance. ¶¶133-34, 201-04. Defendants knew Hamas and PIJ used cryptocurrency to fund their violent aims (¶¶133-37, 201-31); intended that the Binance platform profit from criminal usage and accordingly misled its regulators (¶¶174-92); knew that Hamas and PIJ transacted on Binance (¶¶193-231); and knew that Hamas and PIJ transacted in staggering amounts leading up to the Attacks. ¶¶194-98, 209. Zhao admitted that Defendants' deliberate concealment of terrorist financing could lead to a terrorist attack. ¶221.

That this case concerns cryptocurrency underscores the foreseeability of the Attacks, as cryptocurrency is tailored for terrorists to conceal their financial transactions in support of deadly goals. ¶¶143-44; *see supra* Section I.A.1; *Schansman*, 565 F. Supp. 3d at 418 (proximate cause where financial service entities were indifferent to servicing terrorist intermediaries); *Strauss*, 925 F. Supp. 2d at 432 (same); *Goldberg*, 660 F. Supp. 2d at 430 ("entirely foreseeable" that transmitting money to FTO intermediary "would lead to violence").

Defendants maintain that proximate cause cannot be established unless they directly supported the attacks that caused Plaintiffs' injuries. Mot. 14. But Defendants' assertion fails as a matter of law. *See Miller*, 372 F. Supp. 3d at 46 ("but for" cause "cannot be required"; it "would eviscerate Section 2333(a)."). Plaintiffs are "not required to trace specific dollars to specific attacks." *Strauss*, 925 F. Supp. 2d at 433; *see also Goldberg*, 660 F. Supp. 2d at 429 ("Congress did not intend to limit recovery to those plaintiffs who could show that the very dollars sent to a terrorist[s] were used to purchase the implements of violence that caused harm to the plaintiff.").[6]

III. PLAINTIFFS HAVE STANDING UNDER THE ATA

The ATA provides a right of action to "[a]ny national of the United States injured in his or her person … by reason of an act of international terrorism, or his or her estate, survivors, or heirs [.]" 18. U.S.C. § 2333(a). Courts should "interpret the statute broadly." *Henkin*, 495 F. Supp. 3d at 152. Defendants incorrectly maintain that 18 Plaintiffs lack standing. Mot. 19-20.

[6] Defendants' cited authorities (Mot. 14) are inapplicable. In *In re Terrorist Attacks on Sept. 11,* 2001, the allegations that defendants provided financial services to an FTO's intermediaries were conclusory and implausible, as opposed to the FAC's. *See* 714 F.3d 118, 124 (2d Cir. 2013); *see also Kaplan v. Lebanese Canadian Bank, SAL*, 405 F. Supp. 3d 525, 534 (S.D.N.Y. 2019) (inapposite on primary liability claims because those plaintiffs did not allege how the bank-defendant's customers were affiliated with an FTO); *Zapata* v. *HSBC Holdings PLC*, 414 F. Supp. 3d 342, 358 (E.D.N.Y. 2019) (supports Plaintiffs' position by recognizing that providing financial services to designated terrorist organizations "such as Hamas or front groups for such organizations … definitionally enables them to commit additional acts of terrorism").

The U.S. Citizens Have Standing: Uri Raanan and H.B. have standing; they are U.S. citizens. ¶¶21, 59; Raanan Decl. ¶¶3-6; *see Lelchook v. Commerzbank AG*, 2011 WL 4087448, at *2 (S.D.N.Y. Aug. 2, 2011) (living U.S. plaintiffs could pursue claims); *see also* Appendix A.

The U.S. Decedents' Close Family Members Have Standing: Eran Shani, Susan Troen, Hadassah Troen, Revital Mathias, Amos Semama, and Jeffrey Ludmir have standing because they are the functional equivalent of immediate family of the U.S. citizens murdered in the Attacks. ¶¶22, 31, 32, 35, 40, 42, 53-54; Ludmir Decl. ¶¶2-12; *see Brown v. Nat'l Bank of Pakistan*, 2022 WL 1155905, at *1 (S.D.N.Y. Apr. 19, 2022) ("familial relationship, such as that of a child, parent, spouse, or sibling" of U.S. citizen killed in terror attack have standing); *In re Terrorist Attacks on Sept. 11, 2001*, 2023 WL 2711126, at *5 (S.D.N.Y. Mar. 30, 2023) (damages for functional equivalent of family members); *see also* Appendix A.

The U.S. Decedents' Foreign Family Members Have Standing: Oren Glisko, Liat Glisko, Y.G., Ori Glisko, Sanda Mathias, Yeshayahu Mathias, Tzafrir Mathias, Revital Mathias, Meira Semama, Amos Semama, Dorian Bosi, and Yosef Ben Aderet have standing because they are the surviving family members of U.S. citizens murdered in the Attacks. ¶¶22, 37-47. *See Henkin*, 495 F. Supp. 3d at 153 (the ATA "contains no requirement" that the survivors or heirs of a U.S national killed in a terrorist attack must be U.S. citizens; their nationality "makes no difference"); *see also* Appendix A.

IV. THE COURT HAS PERSONAL JURISDICTION OVER DEFENDANTS

The Court has personal jurisdiction over Defendants pursuant to New York's long-arm statute or, alternatively, pursuant to FRCP 4(k)(2).

A. The Court Has Personal Jurisdiction Pursuant To CPLR 302(a)

CPLR 302(a) authorizes courts to exercise personal jurisdiction "over any non-domiciliary ... who in person or through an agent ... transacts any business within the state," so long as the

cause of action "***aris[es] from***" that transaction. CPLR 302(a)(1). This is a "low threshold." *Corley v. Vance*, 365 F. Supp. 3d 407, 434 (S.D.N.Y. 2019). A "***single act within New York***" is sufficient. *Licci v. Lebanese Canadian Bank, SAL*, 673 F.3d 50, 62 (2d Cir. 2012).

Defendants, by soliciting and servicing customers in New York, including "VIP" trading firms operating in New York, transacted business in New York. ¶¶11, 15, 68-70, 154, 157. Binance's extensive New York activities should be attributed to Zhao because, as Binance's CEO, he supervised and controlled these activities. ¶¶15, 17, 69, 74-75, 174-81, 191, 217, 220-21. *See Chloe v. Queen Bee of Beverly Hills, LLC*, 616 F.3d 158, 164 (2d Cir. 2010) (CPLR 302(a) gives jurisdiction over "individual corporate officers who supervise and control an infringing activity.").

Defendants maintain that Plaintiffs' claims do not arise from Defendants' New York activities because the FAC does not allege that a New York customer funded the Attacks or that Binance operated from New York. Mot. 21. CPLR 302(a) requires no such allegations.

A claim "arises from" a particular transaction "where there is some articulable nexus between the business transacted and the cause of action sued upon." *Sole Resort, S.A. de C.V. v. Allure Resorts Mgmt., LLC*, 450 F.3d 100, 103 (2d Cir. 2006). This nexus is established by "a relatedness between the transaction and the legal claim such that the latter is not completely unmoored from the former[.]" *Licci v. Lebanese Canadian Bank*, 20 N.Y.3d 327, 339 (2012).

The FAC establishes this. The gravamen of Plaintiffs' claims is that Defendants knowingly provided financial services to Hamas and PIJ such that these terrorists transacted millions of dollars leading up to the Attacks, with the Attacks being the reasonably foreseeable consequence of Defendants' services. ¶¶139-246. Defendants' provision of these services was dependent on their business in New York; to become a viable platform and thereby allow Defendants to service Hamas and PIJ, Defendants deliberately sought out and "prioritized" business relationships with

New York-based "VIP" "market maker" customers, whose high-volume trading provided necessary liquidity for the Binance platform to exist. ¶¶11-13, 17, 68-69, 158. Retaining these users was so existential for Defendants that they engaged in a multi-year scheme to deceive regulators about their New York relationships. ¶¶174-81. Defendants relied on similar deceptive practices to hide their New York-based customers as they did to hide their FTO users. ¶¶180-81; *see In re Tether & Bitfinex Crypto Asset Litig.*, 576 F. Supp. 3d 55, 88 (S.D.N.Y. 2021) ("substantial relationship" between defendant's opening New York bank accounts containing U.S. dollar reserves and crypto manipulation claim because existence of reserves "was a critical component of the illicit scheme," and scheme could not have operated with unbacked USDT).

B. The Court Has Personal Jurisdiction Pursuant To FRCP 4(k)(2)

Under FRCP 4(k)(2), a district court may assert jurisdiction over a defendant if (i) the defendant has been served with a summons or waived service; (ii) the defendant is not subject to jurisdiction in any state's courts; and (iii) asserting jurisdiction is consistent with the U.S. Constitution. FRCP 4(k)(2).

All requirements are met for the Court to exercise jurisdiction pursuant to Rule 4(k)(2). Defendants waived service pursuant to a stipulation entered by the Court in March 2024. (ECF 12; "Stipulation"). If New York's long-arm statute does not confer jurisdiction (and it should), Defendants are not subject to jurisdiction within any state. ¶¶65, 142. Defendants do not contend that jurisdiction over them violates due process, waiving this argument.

Defendants maintain that 4(k)(2) does not apply because they never waived service. Mot. 21. But Defendants' assertion should be rejected because it contravenes the explicit language of the parties' Stipulation. ***Defendants expressly waived "any defense based upon the sufficiency of***

service of process …" ECF 12 at 2. That Plaintiffs purportedly cannot assert 4(k)(2) jurisdiction because of a supposed defect in waiver of service ***is*** precisely such a waived defense.

Additionally, Defendants' assertion should be rejected because it runs afoul of guiding caselaw on this exact issue. *See In re ZF-TRW Airbag Control Units Prod. Liab. Litig.*, 601 F. Supp. 3d 625, 698 (C.D. Cal. 2022) (defect in waiver of service ***did "not foreclose Plaintiffs' argument that there is personal jurisdiction over the foreign Defendants under Rule 4(k)(2)***" because the parties' stipulation waiving service and preserving jurisdiction defenses "***simply places Defendants in the same position as if service had been effected properly"***).

Defendants also maintain that the Court cannot exercise 4(k)(2) jurisdiction because the FAC alleges jurisdiction in New York. Mot. 22. But where a plaintiff asserts 4(k)(2) jurisdiction, it is improper to "foreclose[] an argument … that the defendant is subject to jurisdiction in the state in which the court resides." *Touchcom, Inc. v. Bereskin & Parr*, 574 F.3d 1403, 1415 (Fed. Cir. 2009). Precluding this would "not allow plaintiffs to plead jurisdiction in the alternative" and would "conflict[] [with Rule 8 of] the Federal Rules of Civil Procedure." *Id.*; *see* Fed. R. Civ. P. 8(d)(2) ("A party may set out 2 or more statements of a claim … alternatively or hypothetically"). Plaintiffs' assertion of Rule 4(k)(2) an alternative basis for jurisdiction is appropriate. *See RegenLab USA LLC v. Estar Techs. Ltd.*, 335 F. Supp. 3d 526, 555 (S.D.N.Y. 2018) (recognizing argument under 4(k)(2) as alternative jurisdictional basis).[7]

CONCLUSION

For all the reasons set forth herein, Defendants' Motion should be denied.[8]

[7] On a 12(b)(2) motion, a plaintiff must merely "make a prima facie showing that jurisdiction exists." *Licci ex rel. Licci v. Lebanese Canadian Bank, SAL*, 732 F.3d 161, 167 (2d Cir. 2013). Should the Court not so find, the parties' dispute over material jurisdictional facts lays a basis for jurisdictional discovery. Plaintiffs intend to file such a motion.

[8] If the Court grants any part of the Motion, Plaintiffs will seek leave to re-plead pursuant to FRCP Rule 15(a)(2).

Dated: July 12, 2024

Respectfully submitted,

/s/ Jake Nachmani

SEIDEN LAW LLP
Robert W. Seiden
Amiad Kushner
Jake Nachmani
Jennifer Blecher
Dov Gold
322 Eighth Avenue, Suite 1200
New York, NY 10001
(212) 523-0686

PERLES LAW FIRM, P.C.

Steven R. Perles
(*pro hac vice motion to be filed*)
Joshua K. Perles
(*pro hac vice motion to be filed*)
Edward B. MacAllister
(*pro hac vice motion to be filed*)
816 Connecticut Avenue, NW
12th Floor
Washington, D.C. 20006
(202) 955-9055

Attorneys for Plaintiffs

CERTIFICATION OF COMPLIANCE

Pursuant to Paragraph II-D of the Individual Practices of Judge John G. Koeltl, Plaintiffs have complied with all of the formatting rules contained therein. The total number of words contained herein, exclusive of the cover page, certificate of compliance, table of contents, and table of authorities, is 6997 words.

Dated: July 12, 2024

/s/ Jake Nachmani
SEIDEN LAW LLP
Robert W. Seiden
Amiad Kushner
Jake Nachmani
Jennifer Blecher
Dov Gold
322 Eighth Avenue, Suite 1200
New York, NY 10001
(212) 523-0686

Attorneys for Plaintiffs